UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

_____

Ex parte AHMET MURSIT ESKICIOGLU and BILLY WESLEY BEYERS

_____

Appeal 2007-0038
Application 09/763,773
Technology Center 2100

_____

Decided: November 7, 2007

_____

Before KENNETH W. HAIRSTON, LANCE LEONARD BARRY, and
JOHN A. JEFFERY, *Administrative Patent Judges*.

JEFFERY, *Administrative Patent Judge*.

DECISION ON APPEAL

1 Appellants appeal under 35 U.S.C. § 134 from the Examiner's
rejection of claims 1-11, the only claims pending in this application.[1] We
have jurisdiction under 35 U.S.C. § 6(b). We affirm.

_____

[1] The Examiner entered an amendment filed with the Brief cancelling claims
12-20 on Jun. 23, 2006.

STATEMENT OF THE CASE

Appellants invented a method for copying a program with a scrambled content component (e.g., audio/video program) and an encrypted control component (e.g., an Entitlement Control Message (ECM)). The program is received in a recording apparatus and a data item indicating that the program has been copied is attached to the encrypted control component. Finally, the encrypted control component and the data item together are encrypted to generate a nested control component. As a result, every time a scrambled program is copied, its ECMs are encrypted once again. Therefore, the number of times a program has been copied can be determined.[2] Claim 1 is illustrative:

1. A method for copying a program having a scrambled program content component and an encrypted control component comprising:

(a) receiving, in a recording apparatus, said program;

(b) attaching a data item to said encrypted control component, said data item indicating that said program has been copied;

(c) encrypting said encrypted control component and said data item to generate a nested control component; and

(d) recording said program content component and said nested control component.

The Examiner relies on the following prior art references to show unpatentability:

Mandelbaum	US 5,544,246	Aug. 6, 1996
Park ("Park '559")	US 5,689,559	Nov. 18, 1997
Park ("Park '826")	US 5,796,826	Aug. 18, 1998

---

[2] *See generally* Specification 2:39 – 3:8 and 8:28-37.

EBU Project Group B/CA, *Functional Model of a Conditional Access System*, EBU Tech. Rev., Winter, at 64-77 (1995) ("EBU").

1. Claim 1 stands rejected under 35 U.S.C. § 103(a) as unpatentable over Park '559 and Park '826.

2. Claims 2-7 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Park '559, Park '826, and Mandelbaum.

3. Claims 8-11 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Park '559, Park '826, Mandelbaum, and EBU.

Rather than repeat the arguments of Appellants or the Examiner, we refer to the Brief and the Answer for their respective details. In this decision, we have considered only those arguments actually made by Appellants. Arguments which Appellants could have made but did not make in the Brief have not been considered and are deemed to be waived. *See* 37 C.F.R. § 41.37(c)(1)(vii).

OPINION

We first consider the Examiner's rejection of claim 1 under 35 U.S.C. § 103(a) as unpatentable over Park '559 and Park '826. In rejecting claims under 35 U.S.C. § 103, it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness. *See In re Fine*, 837 F.2d 1071, 1073 (Fed. Cir. 1988). In so doing, the Examiner must make the factual determinations set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966).

Discussing the question of obviousness of a patent that claims a combination of known elements, the Court in *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727 (2007) explains:

> When a work is available in one field of endeavor, design
> incentives and other market forces can prompt variations of it,
> either in the same field or a different one. If a person of
> ordinary skill can implement a predictable variation, §103
> likely bars its patentability. For the same reason, if a technique
> has been used to improve one device, and a person of ordinary
> skill in the art would recognize that it would improve similar
> devices in the same way, using the technique is obvious unless
> its actual application is beyond his or her skill. *Sakraida* [*v. AG
> Pro, Inc.,* 425 U.S. 273, 189 USPQ 449 (1976)] and
> *Anderson's-Black Rock*[*, Inc. v. Pavement Salvage Co.,*
> 396 U.S. 57, 163 USPQ 673 (1969)] are illustrative—a court
> must ask whether the improvement is more than the predictable
> use of prior art elements according to their established
> functions.

KSR, 127 S. Ct. at 1740. If the claimed subject matter cannot be fairly

characterized as involving the simple substitution of one known element for

another or the mere application of a known technique to a piece of prior art

ready for the improvement, a holding of obviousness can be based on a

showing that "there was an apparent reason to combine the known elements

in the fashion claimed." *Id.*, 127 S. Ct. at 1740-41. Such a showing requires

"some articulated reasoning with some rational underpinning to support the

legal conclusion of obviousness. . . . [H]owever, the analysis need not seek

out precise teachings directed to the specific subject matter of the challenged

claim, for a court can take account of the inferences and creative steps that a

person of ordinary skill in the art would employ." *Id.*, 127 S. Ct. at 1741

(quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

The Examiner's rejection essentially finds that Park '559 teaches a

method for copying a program with every claimed feature except for

encrypting the encrypted control component and data item to generate a

nested control component. The Examiner, however, cites Park '826 as

4

teaching this feature and concludes that it would have been obvious to one of ordinary skill in the art at the time of the invention to provide such a feature in the copying program of Park '559 to control the reproduction process thereby enhancing security (Answer 3-4).

Appellants argue that Park '826 does not teach or suggest encrypting an already encrypted component together with a data item, in a nested fashion, to generate a nested control component as claimed. Rather, Appellants contend, Park '826 merely encrypts an unencrypted control word (scrambling key) along with an updatable value. Appellants emphasize that upon decryption, the value itself is updated and recorded. According to Appellants, Park '826 merely teaches extracting and updating a value, but does not teach attaching a data item to an encrypted control component, and encrypting the combination to generate a nested control component (Br. 7-10).

Appellants construe the term "nest" in accordance with its ordinary and customary meaning as evidenced by both dictionary and online technical definitions. Specifically, Appellants indicate that the term "nest" means "to fit or place one within another" or "to fit together or within another or one another" (Br. 5; Ev. App.).

The Examiner construes the term "nested" in light of the Specification as "encrypting...already encrypted data." With this construction, the Examiner indicates that Park '826 in Figure 7 teaches two distinct encryption steps: (1) encrypting a "control component" (scrambling key "m") in adder 12, and (2) further encrypting the encrypted control component together with copy information in matrix multiplier 13.

According to the Examiner, this dual encryption technique generates a nested control component (Answer 7-8).

It is undisputed that Park '559 discloses every claimed feature of independent claim 1 except for encrypting the encrypted control component and the data item to generate a nested control component. It is also undisputed that the references are properly combinable. Rather, the dispute in this appeal is whether the combination of references discloses the disputed limitation of claim 1.

The issue before us, then, is relatively narrow: does Park '826 reasonably teach or suggest encrypting an encrypted control component and a data item to generate a nested control component? For the reasons that follow, we answer this question "yes."

Park '826 discloses an apparatus for limiting the reproducible number of a magnetic recording medium. To this end, an input bit stream is scrambled and recorded on video tape and a scrambling key is encrypted together with additional information indicative of a reproducible number remaining, and then recorded on video tape. During playback, a decryption algorithm restores a scrambling key and information on a reproducible number remaining. Using the restored scrambling key, the original bit stream is restored through descrambling. Also, the reproducible number remaining is reduced by one and then recorded on video tape. If the reproducible number remaining is zero, the scrambling key is not restored (Park '826, col. 2, ll. 48-64).

The hardware configuration for implementing the encryption algorithm of Park '826 is shown in Figure 7. As shown in that figure, the

scrambling key ("m")[3] is encoded using generator matrix G to produce the vector mG (note "mG" at output of ECC encoder 11) (Park '826, col. 4, ll. 9-12). Adder 12 then performs an exclusive-OR operation of the vectors mG and $w^{(i)}$ (a vector indicative of additional information pertaining to the reproducible number remaining) to produce a resulting vector $(b^{(i)})^4$ (Park '826, col. 3, ll. 19-20; col. 4, ll. 53-55; col. 6, ll. 62-64). Then, another exclusive-OR operation effectively multiplies this resulting vector $(b^{(i)})$ (i.e., the vector obtained from adder 12) with the matrix R to obtain the encrypted scrambling key $(d^{(i)})$ (Park '826, col. 4, ll. 54-57; Fig. 7).[5]

We agree with the Examiner that this encryption process, in effect, involves successive "encryptions" that effectively result in a "nested" control component. As the Examiner indicates, adder 12 produces the vector $(b^{(i)})$ from the vector mG – a technique that we find not only encrypts the control component, but effectively "attaches" the "data item" (vector $w^{(i)}$) thereto by virtue of the exclusive-OR operation. We reach this conclusion emphasizing that the original "control component" (scrambling key "m") was first encoded via ECC encoder 11 (which we find reasonably constitutes an "encryption")[6] and again operated on by adder 12 (which is also, in effect, an "encryption"). Thus, adder 12 effectively "attaches" the data item (vector $w^{(i)}$) to vector mG – a process that produces vector $(b^{(i)})$. We also agree with the Examiner that matrix multiplier 13, in effect, further

---

[3] Park '826 notes that the scrambling key "m" is a vector (Park '826, col. 3, l. 17).

[4] *See* Park '826, col. 3, l. 21.

[5] *See* Park '826, col. 3, ll. 22-23 (noting that the encrypted scrambling key $d^{(i)}$ is a vector).

[6] In reaching this conclusion, we note in passing that Park '826 actually refers to matrix G as an "encryption key" (Park '826, col. 4, ll. 49-50).

"encrypts" the vector ($b^{(i)}$) by multiplying this vector with matrix R – a matrix that Park '826 refers to as an "encryption key" (Park '826, col. 4, ll. 49-50).

Therefore, by virtue of these successive "encryptions," the control component (m) is, in effect, "nested" within the resultant vector (encrypted scrambling key ($d^{(i)}$)). We reach this conclusion emphasizing that since the control component can be recovered from the resultant vector, it is, in effect, contained or "nested" therein. As such, we find the Examiner's interpretation of "nested" as the encryption of encrypted data reasonable.

We find no error in the Examiner's specific interpretation of Figure 7 of Park '826 with respect to the disputed limitations (i.e., Step (c) of claim 1), nor have Appellants shown any such error. While Appellants are correct that Park '826 updates a value in the *decryption* process of Figure 8, this argument simply does not address the Examiner's interpretation of the *encryption* process of Figure 7 noted above, namely the multiple "encryptions" shown in that figure. Simply put, Appellants' arguments with respect to the updating capability of Park '826 in the decryption process are not germane to the Examiner's specific interpretation of Park '826 -- an interpretation that we find reasonable and, indeed, unrebutted. *See In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992) (noting that if the Examiner's burden is met, the burden then shifts to the Appellants to overcome the prima facie case with argument and/or evidence).

For the foregoing reasons, Appellants have not shown that the Examiner erred in combining Park '826 with Park '559 to arrive at the invention recited in independent claim 1. Accordingly, we will sustain the Examiner's obviousness rejection of that claim.

Claims 2-11

We will also sustain the Examiner's rejections of (1) claims 2-7 under 35 U.S.C. § 103(a) as unpatentable over Park '559, Park '826, and Mandelbaum, and (2) claims 8-11 under 35 U.S.C. § 103(a) as unpatentable over Park '559, Park '826, Mandelbaum, and EBU.

Regarding claim 4, we agree with the Examiner (Answer 8) that when the value of the reproducible number remaining in Park '826 is zero (and thus resulting in not restoring the scrambling key) (Park '826, col. 2, ll. 61-64), such a value reasonably suggests a "never-copy" state.

We also find that the Examiner has established at least a prima facie case of obviousness of those claims that Appellants have not persuasively rebutted. Specifically, the Examiner has (1) pointed out the teachings of the Park references, (2) noted the perceived differences between these references and the claimed invention, and (3) reasonably indicated how and why they would have been modified to arrive at the claimed invention (Answer 4-7). Once the Examiner has satisfied the burden of presenting a prima facie case of obviousness, the burden then shifts to Appellants to present evidence or arguments that persuasively rebut the Examiner's prima facie case. Appellants did not persuasively rebut the Examiner's prima facie case of obviousness, but merely noted that the rejections of claims 2-11 should be reversed since they depend from independent claim 1. For the reasons previously discussed, however, we find this argument unpersuasive. The rejection is therefore sustained.

DECISION

We have sustained the Examiner's rejections with respect to all claims on appeal. Therefore, the Examiner's decision rejecting claims 1-11 is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

<u>AFFIRMED</u>

gw

JOSEPH S. TRIPOLI
THOMSON MULTIMEDIA LICENSING INC
PO BOX 5312
PRINCETON, NJ 08540